T2147-906626-US 3822/JPL(PCT)

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)

Applicant:	Louis GOUBIN et al.
International Application No.:	PCT/FR00/00902
International Filing Date:	7 April 2000
U.S. Serial No.:	To be Assigned
U.S. Filing Date:	December 8, 2000
For:	**METHOD FOR MAKING SECURE ONE OR SEVERAL COMPUTER INSTALLATIONS USING A COMMON CRYPTOGRAPHIC SECRET KEY ALGORITHM, USE OF THE METHOD AND COMPUTER INSTALLATION**

McLean, Virginia

PROPOSED DRAWING CORRECTIONS

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Applicant requests approval of the drawing corrections on Figs. 1 – 4F as shown in red on the attached eight (8) sheets

The proposed corrections only comprise translating the French terms into English and removing the headings "1/8" – "8/8" to conform the drawings to U.S. practice.

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: December 8, 2000

By: _____
Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686

FIG 1

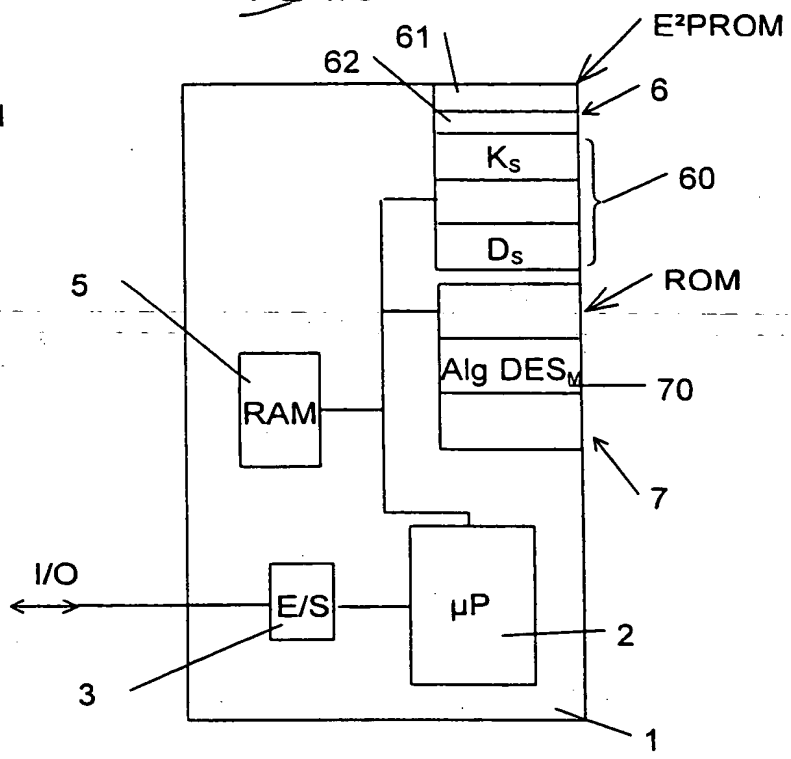
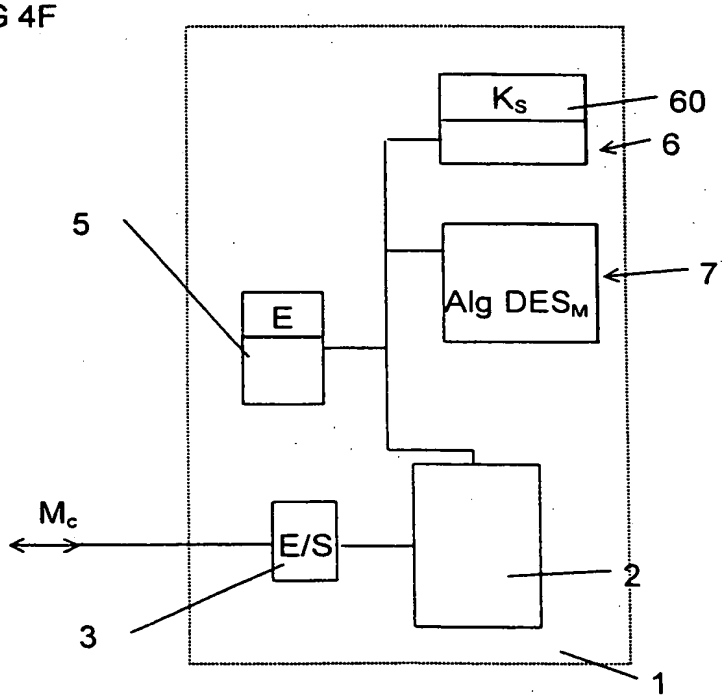

E²PROM
61
62
6
K_S
60
D_S
ROM
5
RAM
Alg DES_M
70
7
I/O
E/S
µP
2
3
1

FIG 4F


K_S
60
6
5
Alg DES_M
7
E
M_c
E/S
2
3
1

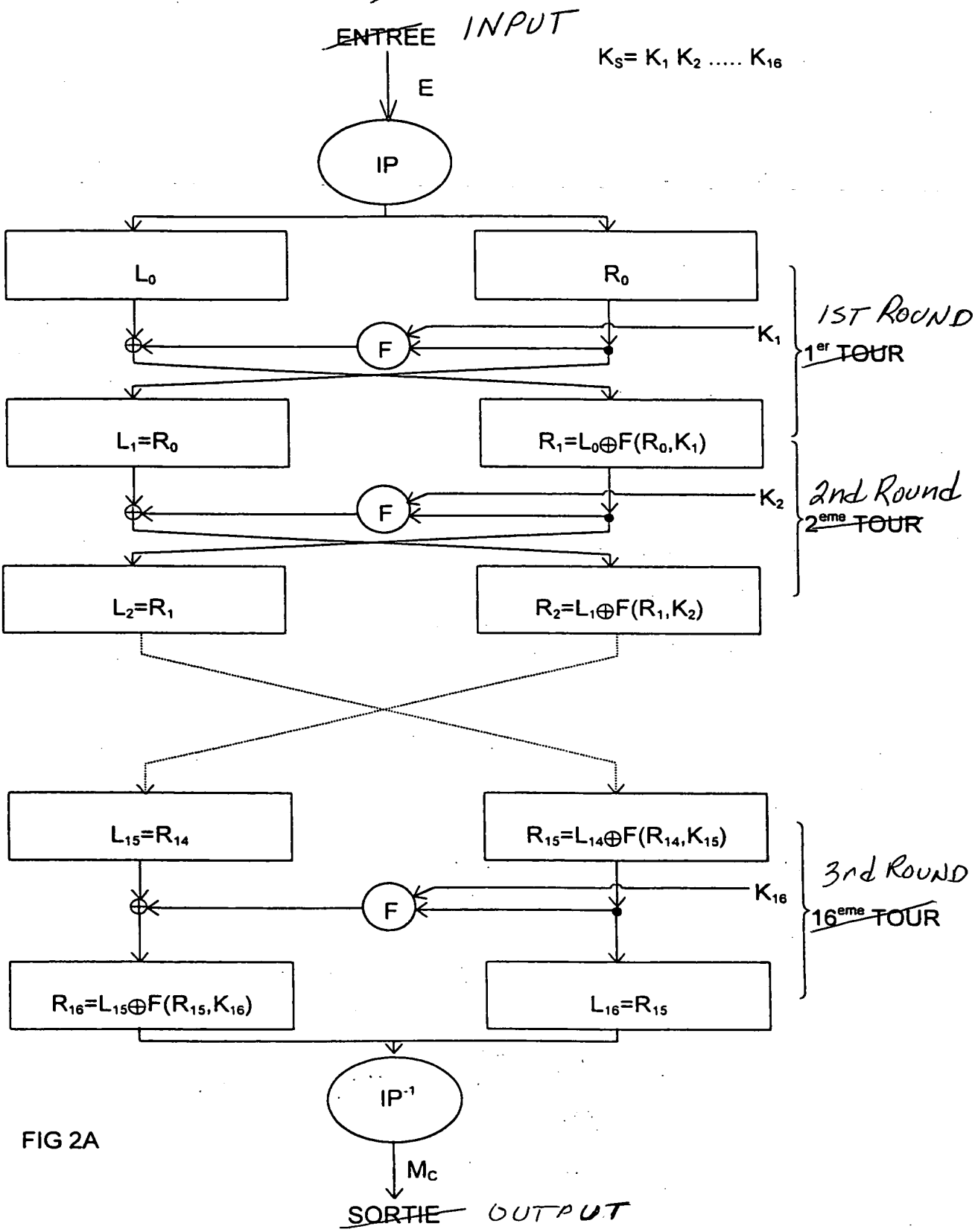

ENTREE
INPUT
E
$K_S = K_1\ K_2\ \ldots\ K_{16}$
IP
L_0
R_0
F
K_1
1ST ROUND
1er TOUR
$L_1=R_0$
$R_1=L_0 \oplus F(R_0,K_1)$
K_2
2nd Round
2eme TOUR
$L_2=R_1$
$R_2=L_1 \oplus F(R_1,K_2)$
$L_{15}=R_{14}$
$R_{15}=L_{14} \oplus F(R_{14},K_{15})$
K_{16}
3rd ROUND
16eme TOUR
$R_{16}=L_{15} \oplus F(R_{15},K_{16})$
$L_{16}=R_{15}$
IP^{-1}
M_C
SORTIE
OUTPUT

FIG 2A

Calcul de $F(R_{i-1}, k_i)$

R_{i-1}

Permutation + Expansion E

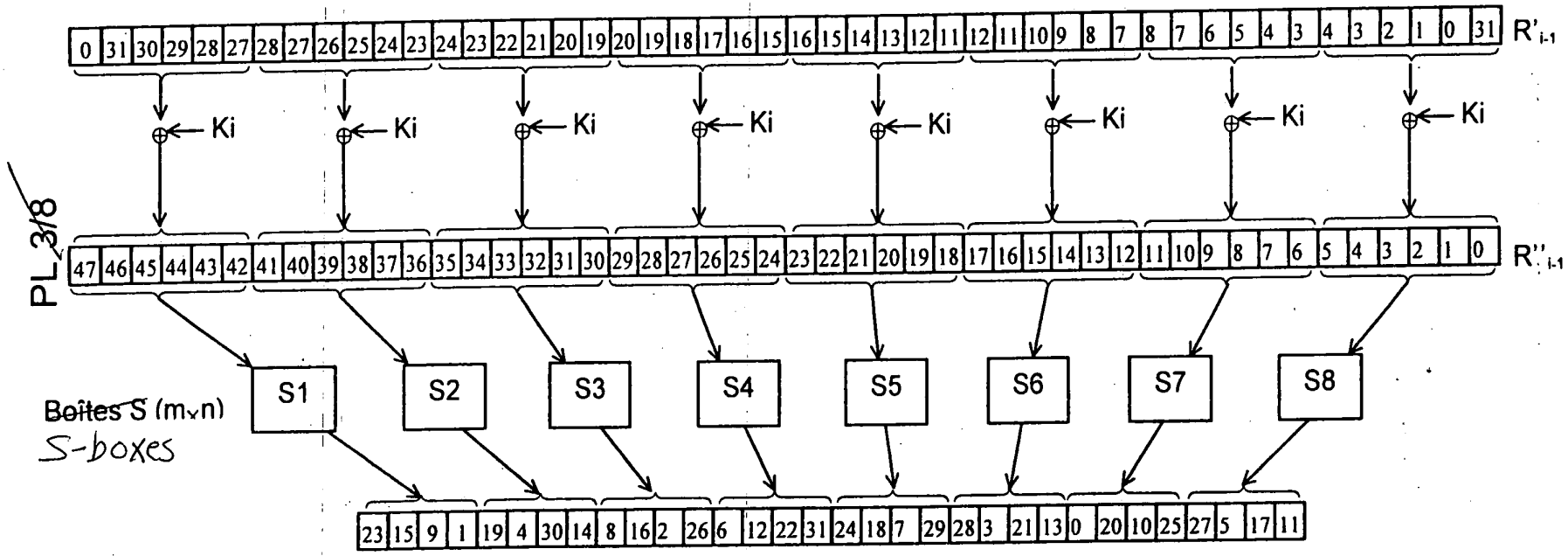
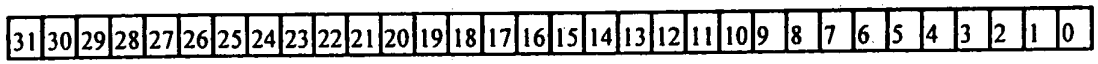


FIG. 2B

Permutation P



$F(R_{i-1}, k_i)$

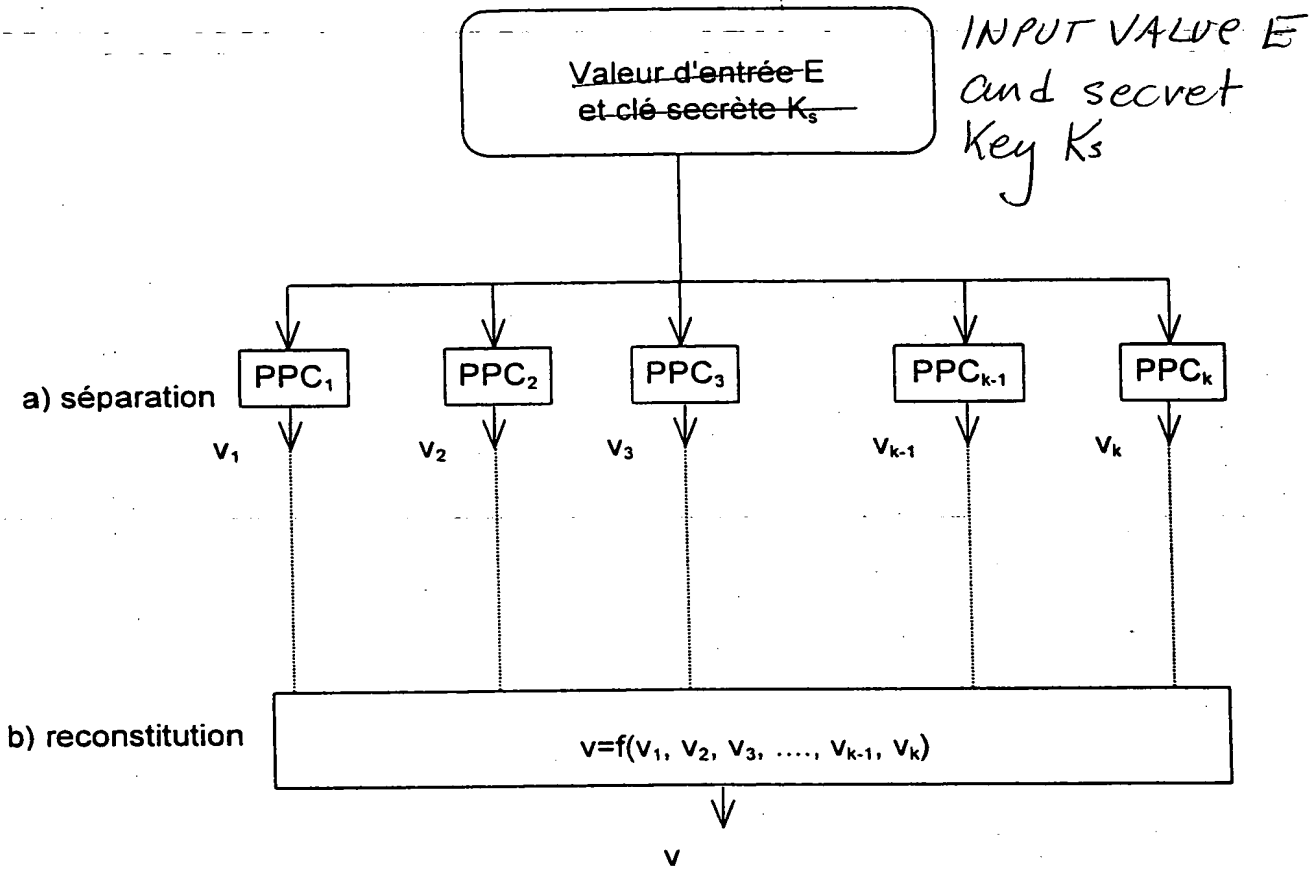

Valeur d'entrée E
et clé secrète K_s
INPUT VALUE E
and secret
Key K_s
a) séparation
PPC_1
PPC_2
PPC_3
PPC_{k-1}
PPC_k
v_1
v_2
v_3
v_{k-1}
v_k
b) reconstitution
$v=f(v_1, v_2, v_3, ..., v_{k-1}, v_k)$
v

FIG 3

PL 5/8

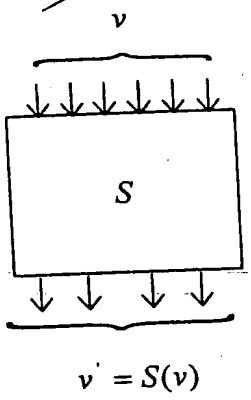


FIG 4A

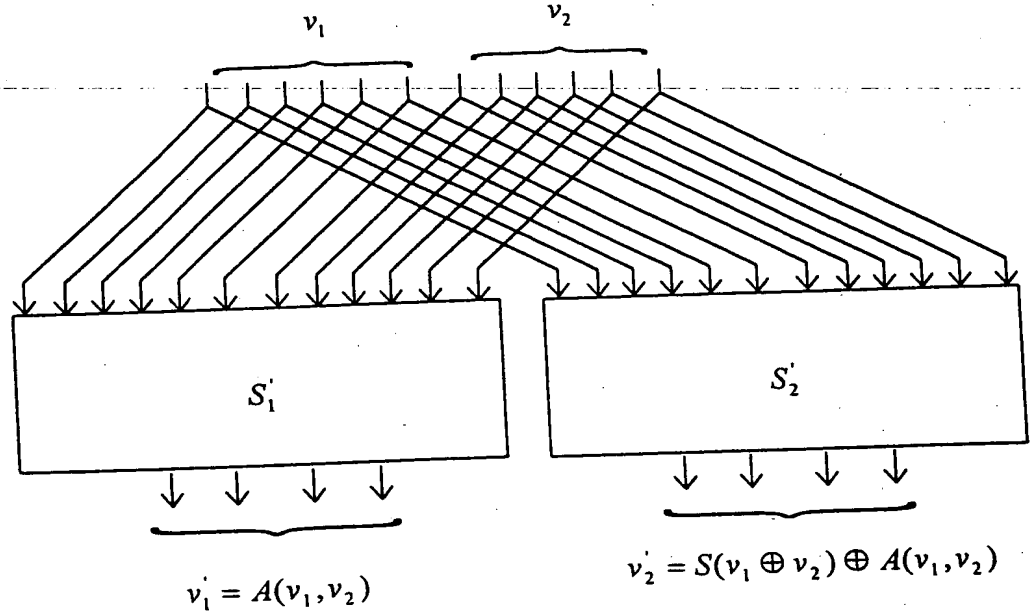


FIG 4B

E

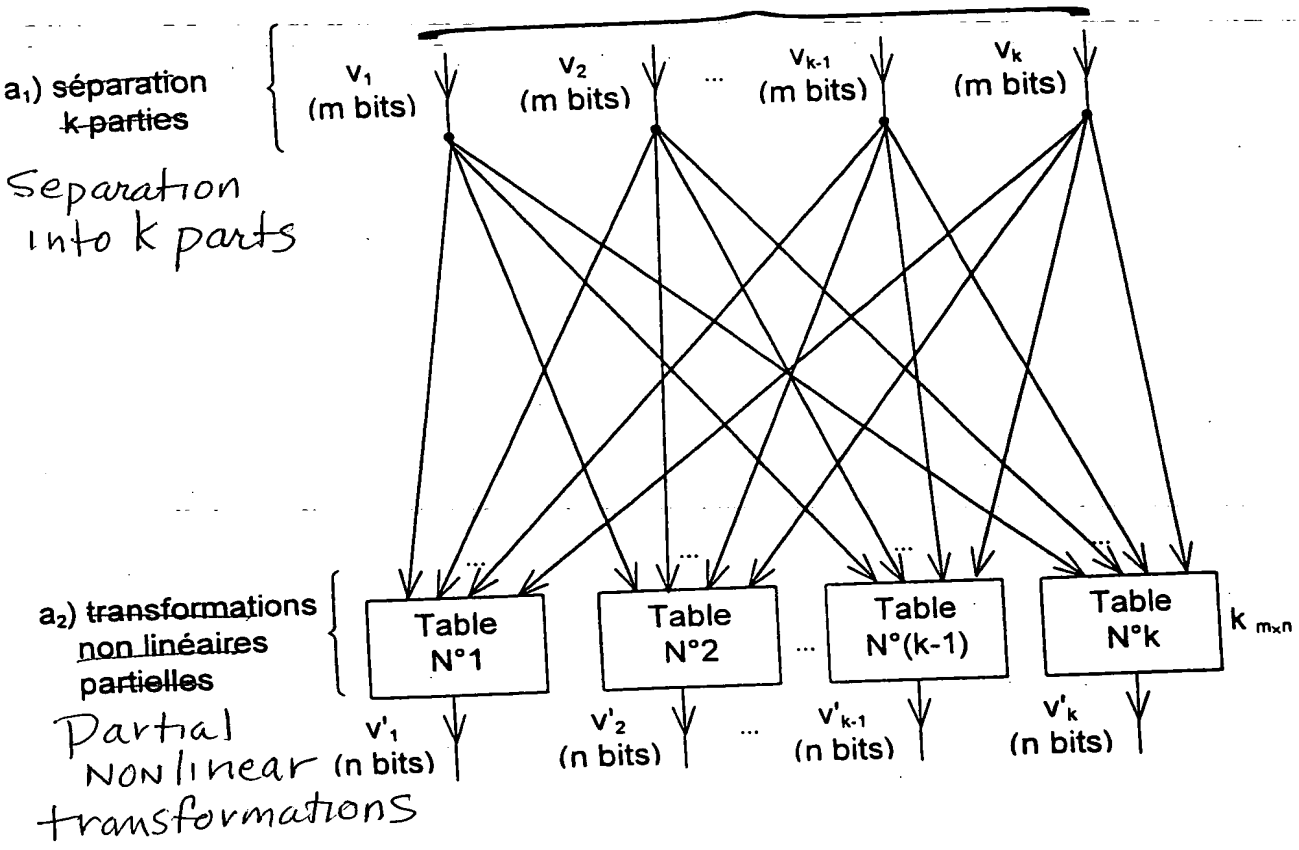

a1) séparation
k parties
Separation into k parts
v1 (m bits)
v2 (m bits)
vk-1 (m bits)
vk (m bits)
a2) transformations non linéaires partielles
Partial NONlinear transformations
Table N°1
Table N°2
Table N°(k-1)
Table N°k
k mxn
v'1 (n bits)
v'2 (n bits)
v'k-1 (n bits)
v'k (n bits)

FIG 4C

PL 7/8

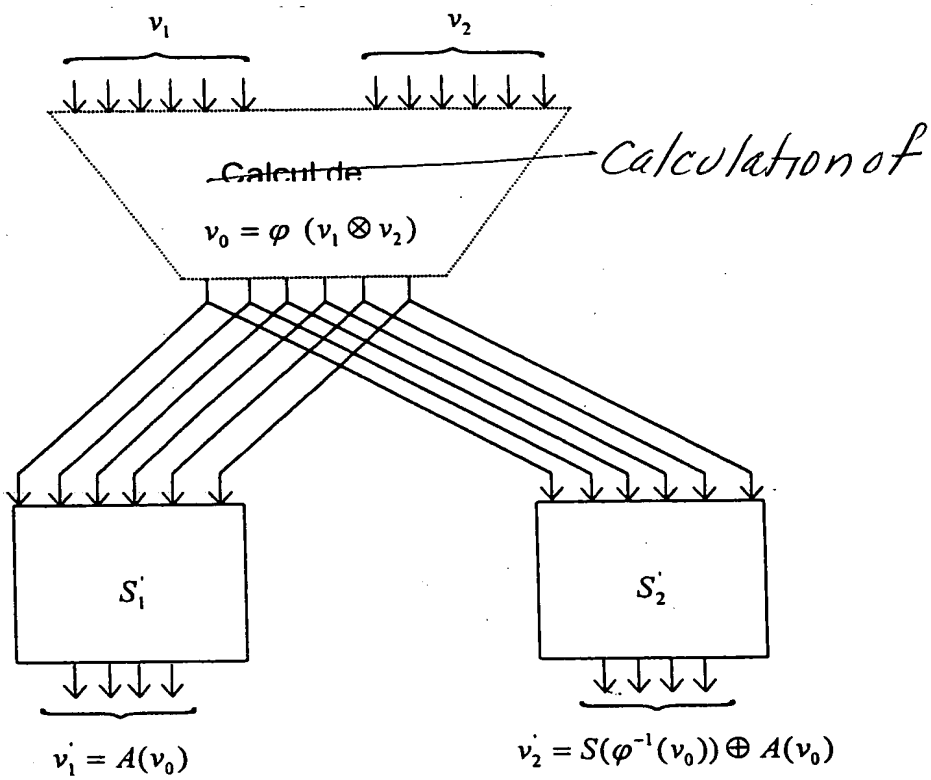

v_1
v_2
Calcul de
Calculation of
$v_0 = \varphi\ (v_1 \otimes v_2)$
S_1'
S_2'
$v_1' = A(v_0)$
$v_2' = S(\varphi^{-1}(v_0)) \oplus A(v_0)$

FIG 4D

FIG 4E